```
id-registeredcert-mg OBJECT IDENTIFIER ::= { id-registeredcert 2 }

id-registeredcert-mg-genminforeq OBJECT IDENTIFIER ::= { id-registeredcert-mg 21 }
id-registeredcert-mg-genpinfores OBJECT IDENTIFIER ::= { id-registeredcert-mg 22 }

GenmInfoReqContent ::= SEQUENCE OF NegotiationKey

NegotiationKey ::= SEQUENCE {
     symmAlg  AlgorithmIdentifier,
     pubAlg   AlgorithmIdentifier,
     hashAlg  AlgorithmIdentifier
}

GenpInfoResContent ::= SEQUENCE {
     status           PKIStatusInfo,
     negotiationKeys  SEQUENCE OF NegotiationKey OPTIONAL
}

END
```

２　Implicitly Tagged Module

```
MOJCRMFCertReq { 1 2 392 100300 1 4 12 }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

        AlgorithmIdentifier
        FROM MOJCMPCertReq { 1 2 392 100300 1 4 11 }

        SubjectPublicKeyInfo, Name, RDNSequence
        FROM MOJCorpCertExplicit { 1 2 392 100300 1 4 1 };

CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg

CertReqMsg ::= SEQUENCE {
    certReq   CertRequest,
    pop       ProofOfPossession }

CertRequest ::= SEQUENCE {
    certReqId     INTEGER,
    certTemplate  CertTemplate }

CertTemplate ::= SEQUENCE {
    serialNumber  [1] INTEGER,
    publicKey     [6] SubjectPublicKeyInfo }

ProofOfPossession ::= CHOICE {
    signature            [1] POPOSigningKey }

POPOSigningKey ::= SEQUENCE {
    algorithmIdentifier   AlgorithmIdentifier,
    signature             BIT STRING }

EncryptedValue ::= SEQUENCE {
    symmAlg       [1] AlgorithmIdentifier,
    encSymmKey    [2] BIT STRING,
    keyAlg        [3] AlgorithmIdentifier,
    encValue       BIT STRING }

GeneralName ::= CHOICE {
    directoryName         [4] Name }

END
```

付録４　休止届の送信の方式（送受信電文の ASN.1 構造とオブジェクト識別子）

１　Explicitly Tagged Module

```
MOJCMPSuspReq { 1 2 392 100300 1 4 21 }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS

      Certificate
      FROM MOJCorpCertExplicit { 1 2 392 100300 1 4 1 }

      GeneralName, EncryptedValue, CertTemplate, CertId, ReasonFlags
      FROM MOJCRMFSuspReq { 1 2 392 100300 1 4 22 };


AlgorithmIdentifier     ::=  SEQUENCE {
   algorithm            ALGORITHM-ID.&id({SupportedAlgorithms}),
   parameters           ALGORITHM-ID.&Type({SupportedAlgorithms}
                                          { @algorithm }) OPTIONAL }

ALGORITHM-ID ::= CLASS {
```